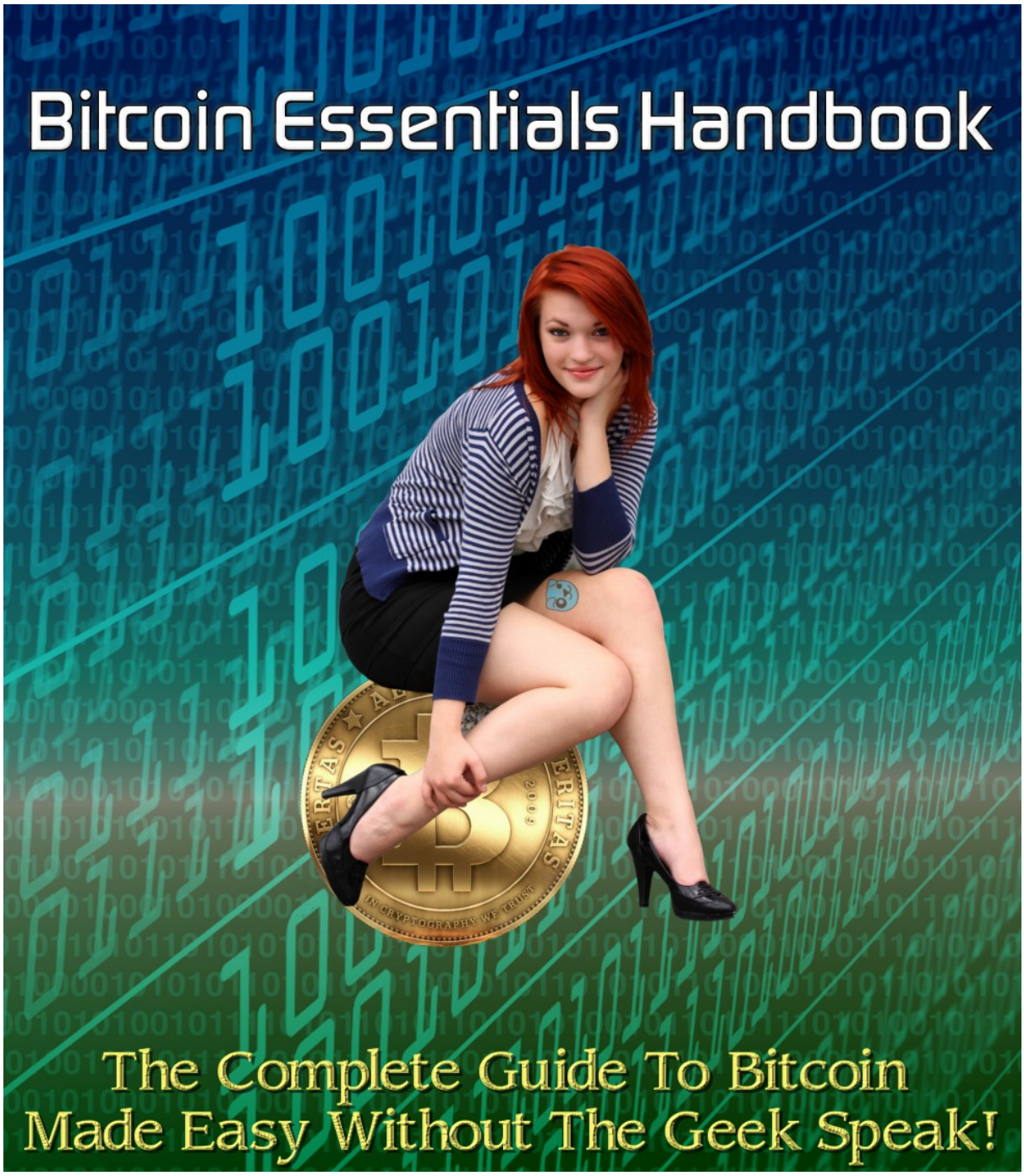


v1.1

2nd Printing, January 2014

Table Of Contents

Attributions & Legal Notices

The *Bitcoin Essentials Handbook* was made possible by the hard work and efforts of countless individuals that blazed the bitcoin trail. I would especially like to extend a warm & hearty “Thank you!” to each of the following for inspiring the very essence of this document:

- Bitcoin.it
- Bitcoin.org
- CoinDesk.com
- BitcoinTalk.org
- DataDealer.com
- WeUseCoins.com
- TheBitcoinWife.com

Legal Notices:

Disclaimer:

This document is not an offer or solicitation for investment advisory services, brokerage or banking services, or other products or services regarding financial services or derivatives trading. **Any views expressed are provided strictly for informational purposes and are purely my own opinions**.

The information contained herein *should not* be construed or interpreted in any way as advice or an offer, an endorsement, testimony, or inducement to invest or trade: Exercise due diligence, and *always seek professional help when it is prudent to do so.*

Copyright Notice:

Redistribution Rights:

Brief Word From The Editor

Hello and welcome to the *Bitcoin Essentials Handbook,* where you're about to discover:

- Bitcoin explained in plain English,
- A simple step-by-step systematic bitcoin approach,
- A plain English explanation of common bitcoin terms,
- How to easily avoid the nasty pitfalls that haunt new bitcoin users,
- The core essentials required to make a well-informed decision on which type of bitcoin wallet / client best meets your needs,
- And lots of great tips and free resources to help keep both you and your bitcoins safe & secure, just to name a few.

So without any further ado, let us now embark upon this most exciting journey into the bitcoin ecosystem!

Your Host,

Mark M. Bravura
UberNifty.com

Bitcoin Explained In Plain Simple English

"In essence, Bitcoin's success is due to the fact that the man in the street understands that central banks and governments are going to take their money via confiscation or default or devaluation and it is their way of voting against it and them (since gold is not easily exchangeable for them).

This is the 99% sticking their fingers up at the authorities and saying we don't need you or want you..."

Raoul Pal
GlobalMacroInvestor.com

So what exactly is bitcoin, minus the techno-BS?

The short answer, is that bitcoin is an experimental, decentralized currency (aka "cryptocurrency") *specifically made for the web*.

Just as email is the digital counterpart of "snail" mail, bitcoin is the digital counterpart of both fiat currency and gold.

Bitcoin enables direct peer-to-peer payments to anyone, anywhere in the world. As such, it bypasses all of the usual headaches and hassles associated with typical online payment processors.

The longer answer, is that bitcoin is an open source innovation based on the mathematics of public-key cryptography. It uses Miners (covered below) to solve what amounts to *complex cryptographic puzzles*.

Bitcoin was originally inspired by an article written in 1998 by Wei Dai that envisioned the concept of cryptocurrency called "B-money". However, it was actually first created by a mysterious individual or group that went by the moniker "Satoshi Nakamoto"; released to the general public in early 2009, under the MIT open source license.

All of the *most respected & trusted* bitcoin wallet derivatives to this day still take an open approach. Also in a similar open manner, bitcoin leverages technology *without the need of a central authority*.

For example, mining new bitcoins and managing bitcoin transactions are carried out collectively by via a peer-to-peer *distributed network* (think along the lines of BitTorrent or Napster).

What this basically means, is that instead of having to trust some third party 'blackbox' faction controlling your fate (i.e. PayPal)... bitcoin is managed over the entire network of it's

user base; hence why it's referred to as a 'distributed network'.

To process, verify and archive payments, bitcoin uses a unique combination of peer-to-peer networking, a public ledger (called a 'blockchain') and a *proof-of-work* protocol (the solving of complex cryptographic puzzles by Miners).

Bitcoins are essentially signed over from one cryptographic wallet address to another. In turn, each payment transaction is broadcast across the network and added to the blockchain.

Provided that the receiver waits for at least 1 Miner confirmation (to ensure that the bitcoins sent are legit)... the same bitcoin is not at all easily spent back to back, twice (called a "double spend"). Each additional confirmation makes it exponentially more difficult to double-spend. Seven confirmations, and that transaction is 'etched in stone'.

If the sender goes ahead and pays the standard minimal Miner fee, the first confirmation usually takes place within 10-20 minutes. Within less than two hours, each transaction is permanently 'locked in time' on the publicly-viewable blockchain (via the massive Miner processing power that continues to strengthen the blockchain).

Consequently, bitcoin provides an open, honest and reliable payment network for everyone in the world. And *unlike* fiat currency (government-controlled, debt-based, inflated "funny money" that can be printed at will)...

Bitcoin can potentially store *real value* over time.

In other words, the most your fiat currency will be worth, is what it's worth *right now*. This is because fiat currency can be printed at the mere whim of the draconian controllers (hence the term "inflation").

This has the *utterly nasty* side effect of making your hard-earned money worth even less than it's already worth. Wash, rinse, repeat... until the inevitable crash.

Whereas the value of one bitcoin has gone from US$0.03 (yes, three pennies) per bitcoin in February 2009, to a peak value of over US$1250.00 (near the end of 2013; momentarily surpassing the price of 1 gold ounce).

According to a *conservative* estimate by Cameron Winklevoss (of the legendary Winklevoss Bros. FaceBook lawsuit), he conservatively estimates that bitcoins will reach at least **$40K** *per bitcoin*. And in early January, 2014, a survey revealed that 56% of Bitcoiners believe bitcoin reach **$10K in 2014**. I am definitely with the positive majority on that prediction!

Bitcoin .vs Fiat & Gold

Unlike *fiat currencies*, bitcoins:

- Not debt-based,
- Are frozen-account proof,
- Are not controlled by a draconian faction (i.e. the Federal Reserve),
- Cannot be inflated, as they are precisely limited in supply (21 million, ever).

Furthermore, *unlike gold*, bitcoins are easy to:

- Store,
- Secure,
- Transfer,
- And convert into smaller units.

Best of all - *like hard cash* - bitcoins are also potentially anonymous (as anonymous as you're willing to make them).

Honest Money

To get a deeper appreciation for the benefits bitcoin offers you and your loved ones, consider the following excerpt from *Bitcoin - What It Is and Why It Matters*, by Anthony Freeman:

"Honest Money (defined as a medium of exchange consisting of real goods that are in limited supply) can actually increase in value over time. Let me explain.

When the production of other economic goods grows at a faster rate than the supply of money (mined gold for example) the money can buy (be traded for) more of these other goods (money supply divided by the total number of goods).

This means that it could actually pay to save your money because it can increase in exchange value over time. This also means that nominal wages could decrease over time while real wages increase (your paycheck "amount" drops but your purchasing power increases).

Why and how did Government Money supplant Gold and Silver? Laziness and deceit. The first bankers were the goldsmiths. Miners would bring the gold to the goldsmiths for minting. The goldsmith would give the miner a receipt that he could redeem when the minting was completed.

The miner soon found that he could immediately trade his receipt (his claim on the gold) for tools and supplies and return to the mines without having to wait for his gold. Over time, the

goldsmith found that the receipts he issued stayed in circulation and were being used as medium of exchange. Only a small percentage of the people ever came in to redeem the receipts.

To increase his purchasing power he simply began to issue his own fraudulent receipts (that had no gold backing) and used them to acquire goods and services. This increase in the number of outstanding receipts created inflation and lessened the value of all of the other outstanding receipts.

In later days, central banks did the same thing. They issued more receipts (paper currency) than they had the gold and silver to back it. The U.S. paper currency was originally a receipt for gold or silver. ”

Isn't it long overdue time to finally *get back to honest money*?!

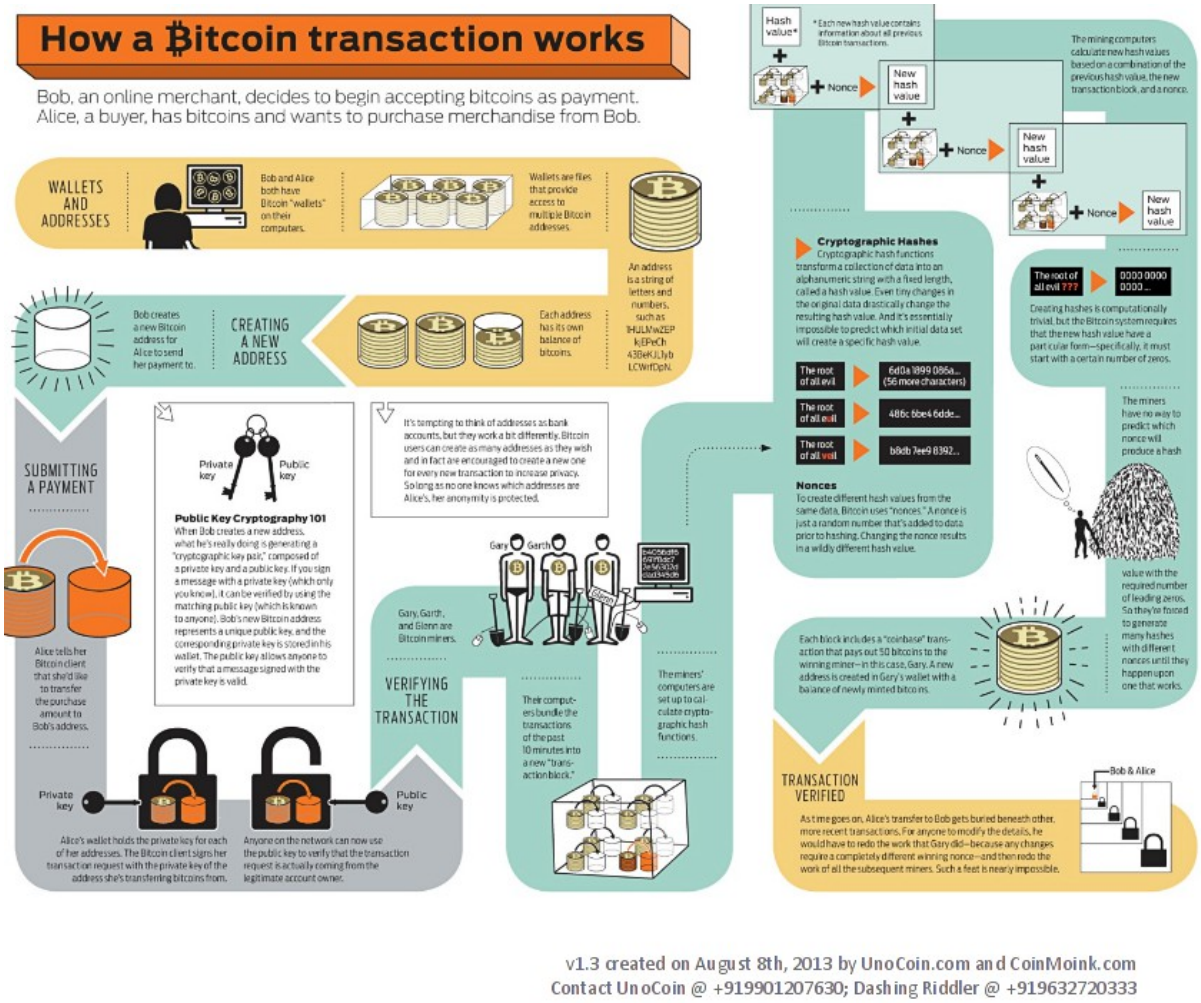
Common Bitcoin Increments

1BTC =

- 1000 mBTC (milliBTC; 0.001 BTC)
- 1,000,000 µBTC (microBTC; 0.000001BTC)
- 100,000,000 satoshis (a satoshi is a bitcoin's smallest divisible unit; 0.00000001BTC)

Visually Understanding Bitcoin

TryBTC.com is truly innovative, as it features *interactive tutorials* (via a nifty online visual bitcoin walk-through). Participants intuitively learn about wallets, addresses, transactions, and the blockchain. You even get a little BTC to experiment with!



v1.3 created on August 8th, 2013 by UnoCoin.com and CoinMoink.com
Contact UnoCoin @ +919901207630; Dashing Riddler @ +919632720333

Attribution: CoinMonk.com/What%20is%20Bitcoin%20-%20CoinMonk.pdf

The Bitcoin Baroness series (starring the legendary Betty Boop) serves to make Bitcoin truly *female-friendly* in a fun, upbeat manner. Enjoy!

Bitcoin Benefits For End Users & Merchants

“The bitcoin protocol provides an *elegant solution* to the problem of creating a digital currency (i.e. how to regulate its issue, defeat counterfeiting and double-spending, and ensure that it can be conveyed safely—without relying on a single authority)...

It represents *a remarkable conceptual and technical achievement*, which may well be used by existing financial institutions (which could issue their own bitcoins) or even by governments themselves.” [Ed. Note: emphasis mine]

The Federal Reserve Bank of Chicago
Chicago Fed Letter , December 2013, No. 317

Bitcoin Benefits For End Users

For end users, the benefits of shopping with bitcoin are *breathtakingly refreshing*:

- **Super simple sending and receiving.** Send bitcoin payments via mobile with a simple two step scan-and-pay. No need to swipe your card, type a PIN, sign anything, or other such tripe.

  To receive bitcoin payments is just as quick and easy: Simply display the QR code in your bitcoin wallet app and let your friend scan your mobile. And with NFC radio technology, it's even easier... just touch the two phones together!

- **Bitcoin transactions are secured by military grade cryptography.** Nobody can charge your wallet or make a payment on your behalf without your consent.

  And provided that you're willing to properly protect your wallet, bitcoin gives **you** *total control over your own money*. Moreover, it also gives you strong protection against many types of fraud.

- **Every bitcoin user gets to stick with their personal favorites.** Just as with email clients, no two bitcoin users are required to use the exact same software or service providers.

  Because they all use the same open technology, they're all fully compatible. Best of all, just like the web itself... t*he bitcoin network never sleeps* (not even on holidays)!

- **Bitcoins can be transferred country to country in less than 20 minutes.** There is no bank to add days to the process, tack on outrageous fees, or freeze the transfer.

  Bitcoin allows you to pay a family member in another country with the same ease as your neighbor next door.

- **Send and receive payments at very low to no cost.** Except for special cases like very small payments, there is no enforced fee.

It is however highly recommended to pay the voluntary Miner confirmation fee for *MUCH faster confirmation of your transaction*. It also has the added benefit of rewarding the people who keep the bitcoin network safe, free, and fair for all.

- **Keep your true identity safe.** With bitcoin, it is entirely possible to send a payment without revealing your personally identifiable information. It's important to note that this highly desirable degree of privacy – *while not necessarily 'difficult'* – will require some effort on your part.

Hot Tip: Be sure to check out the Bitcoin Wiki for an impressive list on *where to buy bitcoin*.

Bitcoin Benefits For Merchants

Attribution: Wikimedia.org

It's no surprise that bitcoins have become a highly desirable payment venue for businesses both large and small. Some of the more prominent features include:

- **No chargebacks.**

  Confirmed transactions are protected by the full hashing power of the network. So businesses can accept bitcoins from any country in the world, with no risk of chargeback fraud. It is up to the Merchant to honor their money-back guarantee.

- **Frictionless spending.**

  Unlike a typical credit card transaction... making purchases is SO smooth with

bitcoin, that it's practically seamless.

- **Total inclusion.**

  With an almost cavalier “no consumer left behind” feel... Consumers in certain countries that cannot obtain a typical bank account, as well as those who've been barred from PayPal will find bitcoin a welcome wonder.

  Likewise, with Merchants who've experienced the brutal torment of PayPal hell.

- **Passionate community.**

  Because bitcoin is still in the pre-mass adoption stage, it does enjoy an *extremely enthusiastic community very willing to business* with Merchants that accept bitcoin.

  Here's a fascinating case example of a business that enjoyed a massive boost in sales once they started accepting bitcoin.

  Meanwhile, BitPay has irrovacably proven bitcoin's massive growth potential *based merely on bitcoin's infant stages of mainstream adoption*.

- **Additional revenue streams.**

  Aside from being used as a stand-alone payment processing solution, bitcoin can also harmonically co-exist side-by-side with any other checkout options a Merchant already deploys.

- **All-in-one solutions are available.**

  Merchants who still want to process fiat orders, yet would like to enjoy the pleasures of accepting bitcoin can now do so in a seamless manner; via centralized (government controlled) solutions such as BitPay and Coinbase.

As a Merchant, there are certain important questions that you should consider before deciding whether or not to deploy a bitcoin / PayPal combination processor :

1. How do I receive the funds?
2. Are there any fees involved?
3. What is my exchange rate risk?
4. How fast are payments approved?
5. How can I see a listing of my sales?
6. How is the exchange rate calculated?
7. Do I get a unique bitcoin address for each transaction?

Hot Tip: A impressive list of available *bitcoin-friendly ecommerce solutions* can be found on the Bitcoin Wiki. Alternatively, you might also strongly consider an uber nifty *open source* innovation that goes by the name of AcceptBit.

Online & Software Wallet / Client Comparisons

Attribution: BitcoinReportByPhoenix.co

Bitcoin Wallets .Vs Bitcoin Wallet Clients

Often times you'll see these two terms used interchangeably on many sites, However, it's important to actually know the difference. All bitcoin wallets simply consist of 2 cryptographic keys:

- A public key (aka "public address"; the one you share),
- A corresponding private key (the one you hide from prying eyes).
- That's it. Nothing more, nothing less, and nothing else.

What many sites mistakenly misrepresent as a 'bitcoin wallet' is actually a **wallet client**. This is an important distinction, because a bitcoin wallet client *can actually have multiple bitcoin wallets*. So in essence, a wallet client can be accurately described as a **bitcoin wallet management system**.

For example, the end user can (*and should*) set up specific wallets for specific purposes. One might be for Shopping, another for Savings, and perhaps another for Retirement. Yet all can be managed from the exact same client.

Online Wallets

These wallets require zero downloading / installing of any type of software, whatsoever.

Pro's:

- **Convenience:** The best attribute of an online client is the sheer convenience of logging in anytime, anywhere and getting your bitcoin on.
- **Ease of use:** Online clients have a negligible learning curve as compared to other types of wallets; specifically designed to get a bitcoin newbie up and running quickly.

Con's:

- **Less secure:** True open source desktop wallet clients, such as MultiBit, tend to offer far greater security. The following case example illustrates this beautifully.

Summary:

- Online clients are generally avoided by *serious* bitcoin users. However the sheer *pleasure* of super quick, easy, and simple online bitcoin wallets is undeniable.

- To experience the undeniable pleasure of an online bitcoin wallet for yourself... your Host definitely recommends BlockChain.info, as they are the most well-established and trusted of all online bitcoin wallets.

  For example, by way of this most unfortunate nefarious mishap... BlockChain.info has actually *proven themselves to be a reputable company* that values it's users.

Software Wallet Client

Software clients are apps that you download / install into your home computer, laptop, or netbook. These are not to be confused with *portable client* apps (covered below).

Pro's:

- **Heightened security:** Genuine *open source* software clients, such as MultiBit (suitable for beginners), Armory (suitable for advanced users only), or Electrum (suitable for intermediate users) provide a very impressive degree of heightened security.

  All three are perfect for typical everyday bitcoin usage. However, both Electrum & Armory can be custom "accessorized" for unique situations.

Con's:

- **Stationary:** Because a software client is downloaded / installed to a specific machine... much of the pleasurable convenience enjoyed via an online client is exchanged for *safety & security*.

  However, having a dedicated netbook (for the sole purpose of a bitcoin wallet / safe) would be a very a reasonable trade-off between security & convenience; without sacrificing any flexibility whatsoever.

- **Learning curve:** To unlock either Electrum's or Armory's Real Power, there's a substantial learning curve involved.

  Armory's learning curve is definitely far steeper than that of Electrum, which is considerably steeper than that of MultiBit (albeit not necessarily 'difficult').

Summary:

- The MultiBit, Electrum & Armory bitcoin wallet clients are all ideally suited to the serious bitcoin user / investor who values safety and security above all.

- MultiBit is definitely the most user-friendly software wallet client for bitcoin newbies.

- Electrum helps insure against this type of Bitcoin Ugly and is a *good balance* between ease-of-use, learning curve, & flexibility.

- Armory offers the greatest flexibility; albeit at the expense of also having the steepest learning curve.

Portable Wallet Apps

A portable wallet client is a client that is either 1) a stand-alone executable that require no installation on the host computer, or 2) an app made for a mobile device such as an Android or iPhone.

Pro's:

- Mobile portability / convenience.

Con's:

- By far the riskiest / most unsafe of all the different bitcoin wallet / client types.

Summary:

- Your Host recommends that you go with a BlockChain portable wallet app, which is *far less risky* than most mobile wallet apps. At least they're willing to replace your stolen bitcoins.

Overall Conclusion

To enjoy the ”best of both worlds”, your Host recommends starting out with the simple pleasures of an online BlockChain wallet (which can conveniently be integrated with MultiBit).

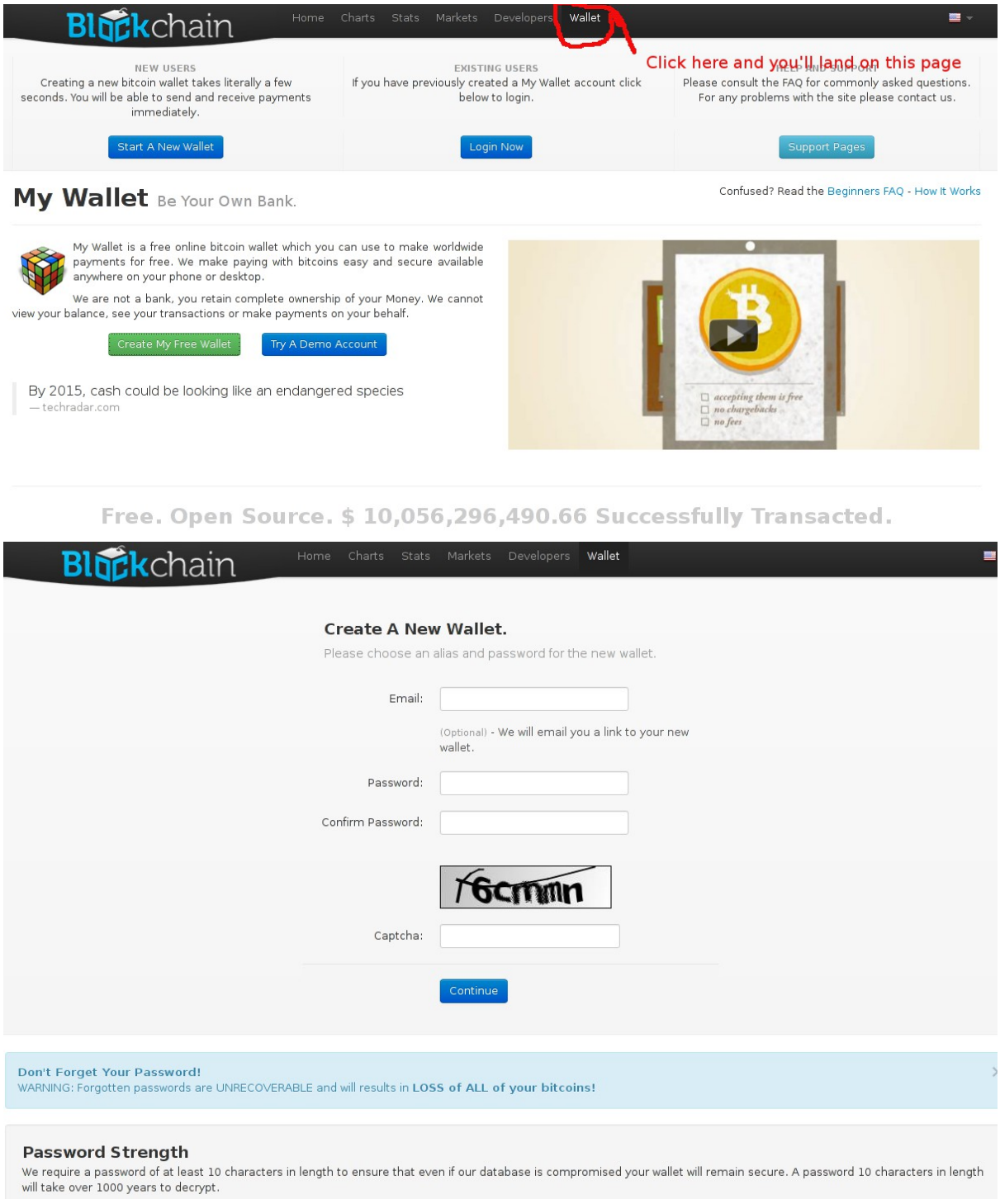
Then, after you've become comfortable with your BlockChain wallet... It's the perfect time to don either the MultiBit or Electrum software client (based on which best suits your particular needs).

Ultra Easy Bitcoin Wallet Tutorial

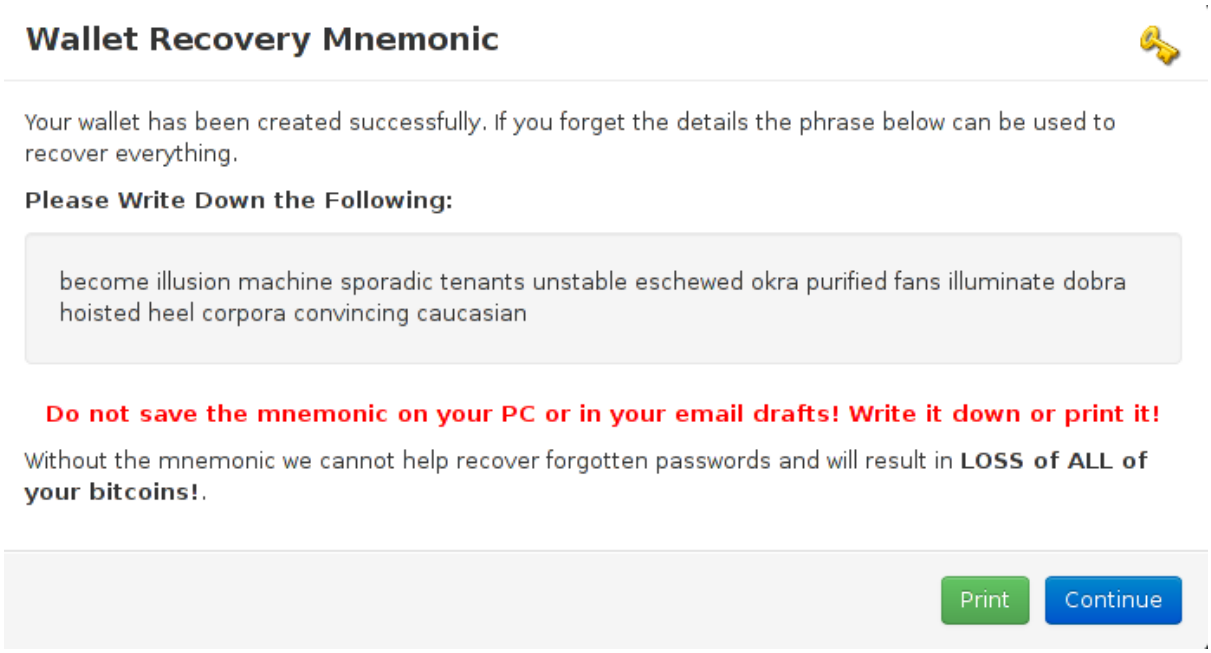
The BlockChain wallet is the perfect balance between *reputability, security and convenience*. And it's a breeze to set up. Here's a completely bogus demo wallet to show you how easy:

Step 1: Go to BlockChain.info and click on the wallet link at the top.

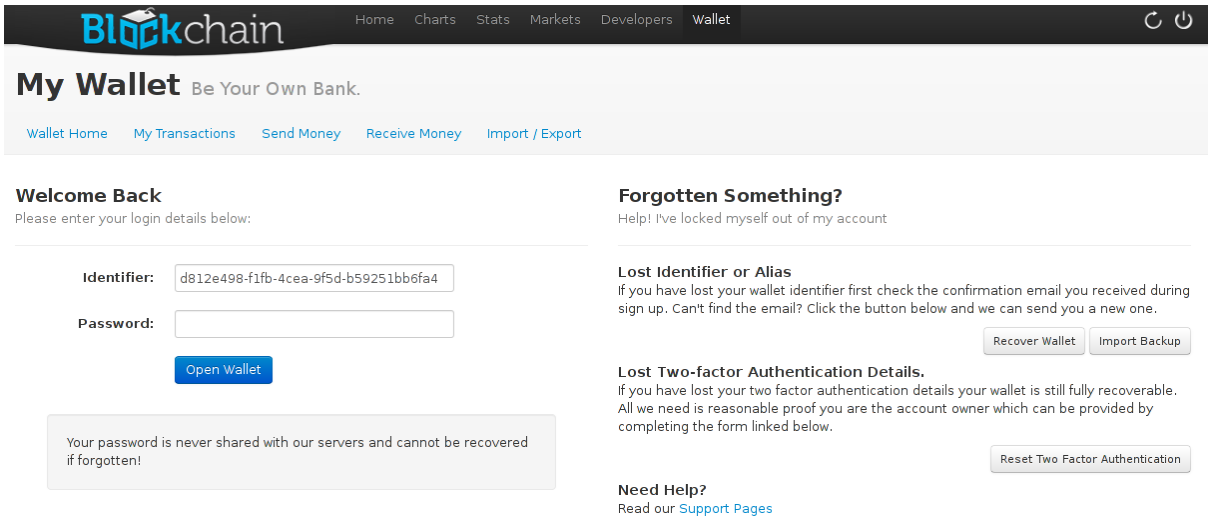
Step 2: After landing on the “My Wallet” page, click the green button pictured below.



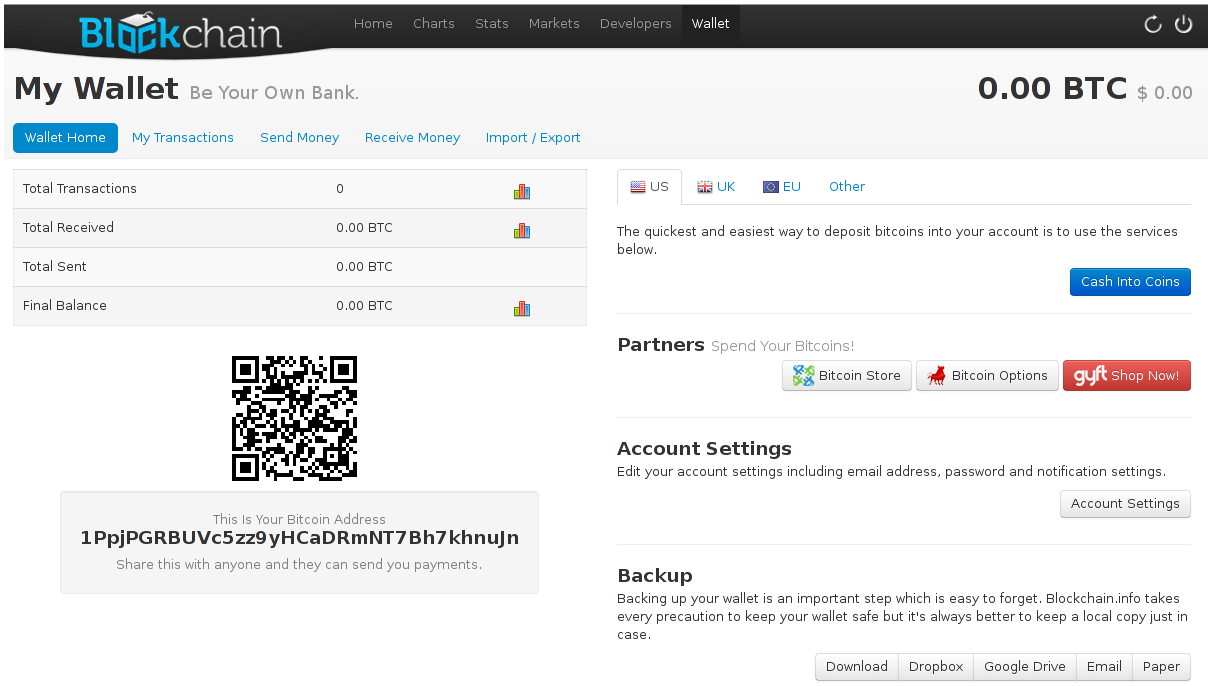
Step 3: Jot down or print out your wallet recovery mnemonic.



Step 4: Log in.



Step 5: After logging into your wallet for the 1st time, click on the “account settings” button pictured below and set up 2-factor authentication for maximum security.



Step 6: Start experiencing the *undeniable pleasures* of bitcoin!

Ultimate Bitcoin Shopping Strategy Unveiled

Brief Introduction

The following shopping strategy invokes an ancient concept most commonly referred to as **arbitrage** (and specifically a term I personally coined: *Bitcoin Shopping Arbitrage*). Now before we dive right into this tender, juicy bitcoin goodness... first, a brief understanding of arbitrage and three indisputable facts about bitcoin are in order.

According to Dictionary.com, arbitrage is defined as:

> *"The simultaneous purchase and sale of the same securities, commodities, or foreign exchange in different markets to profit from unequal prices."*

Perhaps you've heard the saying buy low, sell high. In essence, this is a rudimentary form of arbitrage.

Typically speaking, arbitrage involves making a profit on a difference in prices. For example, if you were to pick up a rare collectible at a yard sale for $1.00, and then turn around and sell it on eBay for $10.00... that would be *eBay arbitrage*.

However, to really appreciate why Bitcoin Shopping Arbitrage will *revolutionize the way people shop* (especially online), we first need to agree on...

Three Indisputable Facts About Bitcoin

- **Fact #1:** Since Feb, 2009, bitcoin has overall gone up 1000's of times in value, and has peaked at over $200 multiple times (in early December 2013, it even briefly overtook the price of gold).

- **Fact #2:** Bitcoin is here to stay, and is gaining in popularity & wider acceptance by the day.

- **Fact #3:** The more popular / widely accepted bitcoin continues to become, the more bitcoin's value will continue to *increase over time*.

As to Fact #3, this scales ever-faster as more counties follow Canada's & Finland's lead by installing their own bitcoin ATM's (scheduled to hit America early 2014). Then, an even *more exciting 'upward spiral effect' happens*, as physical bitcoin hardware wallets go mainstream via *mass production.*

Most exciting of all, however, is the 'quantum leap' that will occur **both** *independent of* **and** *together with* these two separately intertwined events: When *Ladies from the world over take to bitcoin en masse*.

Ok, now that we've established a basic understanding of arbitrage, and three indisputable facts about bitcoin... On with the good stuff!

Bitcoin Shopping Arbitrage

The core concept is actually quite simple. The applications, on the other hand, are *breathtakingly exciting* to say the least. First off, it is absolutely crucial that you:

- Set aside any predispositions concerning Bitcoin;
- Particularly in regards to bitcoin's instability / volatility being a “bad”' thing.

In a nutshell Bitcoin Shopping Arbitrage involves only using bitcoin **for purchases that would clearly give you a distinct financial advantage** (in terms of savings) over using fiat for that exact same purchase.

In the following example, I will use only round numbers so that you can *follow along with the principles* behind what I am teaching:

Let us assume that today, you purchase your first 5 bitcoins ever @ USD$200.00 each. Let us also assume there's really beautiful ring you've had your eye on, priced @ USD$500.00 (which includes shipping, for sake of example).

If you were also to buy that ring today (right after purchasing your bitcoin), it would cost you 2.5 BTC. Therefore, as compared to the price you bought your bitcoins, there would be no net gain, and no net loss; whether you purchased the ring with fiat or BTC.

However, being the super savvy shopper that you are, you *do not* rush right out to spend your bitcoins... but instead decide to sit on them for a bit (and decide not to purchase that exquisite ring *just quite yet*).

As luck would have it, the very next day, Bitcoin shoots up to $250 / bitcoin. However, the website you discovered that beautiful ring on is still offering the ring for your choice of USD$500.00 -OR- *the fair-market equivalent in bitcoin* (according to the most current Mt. Gox trade price, in this case).

Because your bitcoins are (at the moment) now worth $250 / BTC... that same $500 ring (fiat value) will only cost you 2 BTC, instead of the 2.5 BTC you'd have paid the day before. This amounts to a **net gain of $100 in savings**.

And as the Ladies know... a penny save is a penny earned! That is Bitcoin Shopping Arbitrage, in a nutshell. It will work for any product or service, via any fiat / BTC price comparison shopping.

Undiscovered Real Wealth

However, do not let the ease of Bitcoin Shopping Arbitrage fool you. This is *undiscovered real wealth*, pure and simple. How so? A truly savvy and patient shopper willing to...

- Watch the price of bitcoin like a hawk,

- Shop the bargains (i.e. coupon codes, etc.),
- Always buy bitcoins when there's a dramatic price drop,
- And allow her bitcoins to rise back to a really nice level (compared to the *running average* of what she purchased them at)

...could easily double, perhaps even triple her buying power over the course of a month.

Think about that. And even if you only got an extra 20-50% gain in purchasing power, is that alone not *well worth applying these principles*? You bet it is!

It simply does not matter whether bitcoins go up or down in price. How so? Assuming you are willing to keep a **detailed ledger** of your total Bitcoin acquisitions (preferably in a physical paper notebook)...

Then your chances of always coming out ahead (i.e. winning) are *overwhelmingly in your favor.* To qualify that last statement, it is made on the following Foundational Premises:

- The *Three Indisputable Facts About Bitcoin* (covered above),
- Your *well-disciplined willingness to remain patient*, and **only shop with bitcoin when it is lucrative to do so** (as compared to shopping with fiat). Likewise for purchasing more bitcoins.

Hot Tip: Rather than trying to keep track of the price of each and every bitcoin you purchase... this is why you only need to **keep a running average**.

In other words, you'll end up acquiring different amounts of BTC on different days. The only important number to keep track of, is the overall (cumulative) average of your how much your bitcoins cost you on a per-unit basis over time.

For example, let's say you bought 1 BTC a day, three days in a row. Day 1 BTC price = $90, day 2 BTC price = $100, day 3 BTC price = $110. Therefore your "running average" price per Bitcoin is $100.

This makes it really easy to figure out whether purchasing in bitcoin or fiat is the better deal.

Understanding Bitcoin Mining Made Easy

Whenever the you hear the term 'Miner' (as specifically applied to bitcoin), it can mean one of three things... *all of which are completely interchangeable* for practical purposes. A Miner describes:

- The individual doing the bitcoin mining,
- The hardware configuration doing the mining (aka “mining rig”).
- A piece of software that is created for the purpose of solving complex cryptographic puzzles, via a *proof-of-work* model.

Bitcoin uses the Hashcash proof of work, which is based on collecting data in a manner that is:

- Costly (in terms of the computing power required, and electricity consumed),
- And time-consuming (in terms of puzzle difficulty, which *increases by orders of magnitude over time* as more bitcoins are mined).

To this day, many people still falsely believe that Miners are guilty of excessive resource waste in their lust for virgin fresh, new bitcoins.

The fact of the matter, is that Miners *play a critical role in keeping bitcoin a fair ecosystem* by confirming each transaction that enters on to the blockchain. Once a transaction is confirmed on the blockchain, it becomes “etched” in time.

In other words, Miners confirming bitcoin transactions is the *absolute safeguard against double spending spiraling out of control* (via unscrupulous bitcoinsters). For small bitcoin transactions, one confirmation is sufficient.

However, an impressive large transfer (of say 100 BTC) would be wise go with additional confirmations.

Conversely, the more confirmations required... *the longer it'll take for a transaction to clear*; albeit with the benefit of making double spending practically impossible. Interestingly, this can be (somewhat) offset by “tipping” the Miners with a confirmation fee greater than the standard confirmation fee.

Nonetheless, the proof of work supplied by Miners is also what allows them to be *rewarded with new bitcoins*. Whereby slowly growing the bitcoin supply over a very long period of time.

A more commonplace example of how this proof of work concept is put to good use, is as a method to help prevent email spam. For example, requiring a specific proof of work on every email such as the To and From address fields.

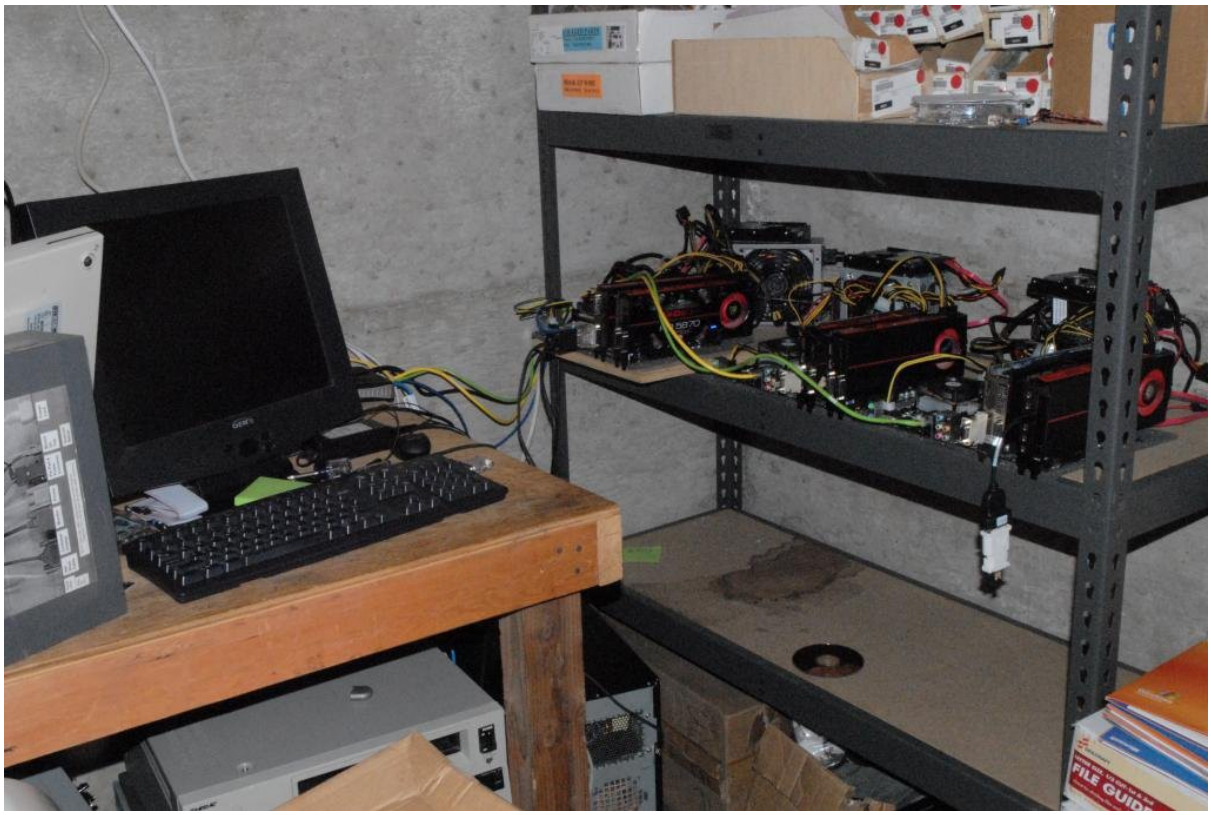
Legitimate emails will be able to do the work (generate the proof easily), as very little work is required for a single email. However, mass spam email blasters will have great difficulty generating the required proof.

Consequently, this results in huge computational resources and energy consumption to provide the necessary proof of work; whereby making it *extremely costly for spamsters*.

In the case of bitcoin, Hashcash proof of work is used in bitcoin for *block generation*. The blocks generated produce a specific amount of bitcoins per block.

As time marches on, each block requires vastly more computing power. Yet the rewards continue to get smaller and smaller per block. In all cases, the difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network.

Bitcoin Mining Rig



Attribution: Bitcointalk.org/index.php?topic=7216.0https://bitcointalk.org/index.php?topic=7216.0

Fascinating Bitcoin Trivia

- There are only 21,000,000 million bitcoins ever to be mined,
- A new block can only be generated *once every 10 minutes* (regardless of how many miners are mining).
- The number of bitcoins mined per block changes every 4 years and yields *only half* of the bitcoins a block previously yielded,
- At the time of this writing, the current yield is 25 bitcoins per block,

- The next time blocks will be halved is 2016,
- The last bitcoin will be mined in 2140.

Due to the extremely low probability of successfully generating a new block, this makes it unpredictable which worker computer in the network will be the one to generate it. Hence why each new block discovery is likened to a “Miner Lotto”.

A solo Miner could mine for a month straight and produce nothing. Yet another Miner might get lucky and hit a new block within a week. It is for this reason that Mining Pools have become wildly popular.

It's not so much that you'll make 'more' being enrolled in a Mining Pool (actually a little bit less, as the Pool Operator receives a fee for Pool maintenance)... but rather that you'll get paid *far more often*; based on the proof work provided by **your** mining rig.

How The Blockchain Got It's Name

For a block to be valid, it must hash to a value *less than* the current target. This means that these blocks have proof that work has been done on it. Each of these blocks contains the hash (a cryptographic *signature* of sorts) of the preceding block.

Consequently, each block has an associated chain of blocks that, when combined, contain a large amount of work.

FYI: Due to the fact that changing a block (which can only be done by making a new block containing the exact same predecessor) requires *regenerating all successors* **and** *redoing the work they contain...* is what protects the blockchain from becoming violated.

It's absolutely important to understand that most bitcoin users **do not mine**. Bitcoin mining is an *investment*, considered by many to be a risky (highly competitive) business. Mining only makes sense in one of two circumstances:

- You do it purely or fun (like going to a casino for an afternoon, not at all concerned with whether or not you win),
- Or you do it most definitely for a profit (i.e. no piddledinking around in the middle).

If it is for the latter reason, you can break into a reasonably decent starter litecoin mining rig for under $2K *provided that you shop around* (litecoin is bitcoin's “kissin' cousin” altcoin and 2nd most popular global cryptocurrency in 2013).

However, *to competitively mine actual bitcoin, itself...* simply plan on shelling out a **respectable five figures**. For more information (including an informative video presentation on Mining), be sure to check out BitcoinMining.com.

Tight Bitcoin A.S.S. (Anonymity & Security Strategy) Tips

Overview

Bitcoin makes it possible to transfer value anywhere very easily. It also allows you to be in control of your money. Such great features also come with great security concerns. However, bitcoin can provide very high levels of security *if used correctly*.

As with the offline world, it is *your responsibility to adopt good practices* in order to protect your money. What follows is numerous tips to keep your bitcoins where they belong – in YOUR possession.

Bitcoin Safety & Security Tips

- **Treat your bitcoins like hard cash.** A bitcoin wallet is like a physical wallet with hard cash.

  As such, it is best to keep only small amounts of bitcoins on your web-enabled computer or mobile device (for everyday use) and the majority of your funds in a more secure cold storage / offline environment.

- **Choose your online wallet or mobile wallet app carefully.** Most online wallet services and mobile wallet apps seriously lack adequate insurance and security.

  For example, an online wallet service that offers two-factor authentication will help to increase the security of your accounts. As with the 1st tip, a more robust offline / cold storage bitcoin solution would better suit substantial bitcoin storage.

- **Back up your wallet.** A safely-stored backup of your wallet can protect you against computer failures and many human mistakes.

  It can also allow you to recover your wallet in the unfortunate event that your mobile device or computer is stolen (if you *keep your wallet encrypted*).

- **Back up your entire wallet.** Some wallet clients use many hidden private keys internally.

  Having a backup of only your visible bitcoin address private keys might not be enough to recover all of your funds.

- **Encrypting ALL of your wallet backups is always wise.** Encrypting your wallet app allows you to set a password against attackers trying to steal your bitcoins.

  Howsoever, it is important to note that it cannot protect you against *keylogging attacks*. Also, any backup that is either stored online or on a computer connected to the web is highly susceptible to theft (i.e. via malicious software attacks).

- **Always remember your password.** You should make sure you never forget the password or your funds will be permanently lost. Unlike your bank, there are very limited password recovery options with bitcoin.

  Certain wallet solutions assign mnemonics in the form of a random string of words (i.e. the BlockChain.info online wallet, and the Electrum software wallet client). This can be *extremely helpful* in the event of wallet recovery.

  However, you should still be able to remember your password *even after many years of not using it*. If in doubt, keep a hard copy of your password in a safe place like a vault.

- **Always use strong passwords.** Any password that contains only letters and numbers or contains any recognizable words is considered very weak (i.e. easy to crack).

  A strong password must contain **at least** one lowercase and one capital letter, one number, and one special character -AND- must be at least 16 characters long, with absolutely *no recognizable words in it*. Take care in memorizing it and archiving it.

- **Two locations are better than one.** If your backup is in multiple locations, it is less likely that you'll be prevented from recovering your wallet. Consider using different storage media types (i.e. USB sticks, physical paper, CDs, etc.)

- **Offline wallets are best for long-term saving.** Offline wallets (aka 'cold storage', such as paper wallets, Electrum & Armory) provide the highest level of security for long-term saving.

  It entails storing a wallet in a non-web-connected manner. When done properly, it can offer *excellent protection* against a wide range of web-connected computer vulnerabilities.

- **Keep your wallet software up to date.** Help keep your wallet safe by using the latest version of your bitcoin software. This arms you with important stability and security fixes (as well as any new features introduced).

- **Consider your loved ones.** Your bitcoins *are lost forever* if you don't have a backup plan for your next of kin. If the location of your wallets or your passwords are only known to you when you pass there is little to no chance of recovering your funds.

Bitcoin Anonymity & Privacy Tips

Perhaps you've heard the media hype about bitcoin being 'anonymous'. Actually, that's only half true. And as we all know: "*Half a truth is still a lie.*"

In reality, bitcoin is probably the most transparent payment network in the world. At the same time, bitcoin can provide impressive levels of anonymity & privacy *when used correctly*.

That said, there are privacy concerns that are well within your control, and others that aren't (albeit being proactively worked on).

It's all about being *exceptionally discreet* when attached to the web in any way whatsoever. Even when you're logged in and not really doing anything. Along the same lines as the extra precautions you'd take when doing online banking... bitcoin is just as serious.

What follows is some great tips to enhance your anonymity and privacy.

- **Understand bitcoin traceability.** bitcoin works with an unprecedented level of transparency that most people are not used to dealing with. All bitcoin transactions are public, traceable, and permanently stored in the bitcoin network.

  Conversely, bitcoin addresses are the only information used to define where bitcoins are allocated and where they are sent. These addresses are created privately by each user's wallets.

  However, once addresses are used, they become tainted by the history of all transactions they are involved with. Moreover, anyone can see the balance and all transactions of any address.

  Since users usually have to reveal their identity in order to receive offline services or goods, bitcoin addresses cannot remain fully anonymous under this circumstance.

  It is for these reasons that bitcoin addresses should *only be used once* and users must be careful not to disclose their addresses.

- **Use new addresses to receive payments.** Hand in hand with the above tip, *you should use a new bitcoin address each time your receive a new payment*. (including any change owed to you - covered below).

  Additionally, it is wise to *use multiple wallets for different purposes*. Doing so allows to isolate each of your transactions in such a way that it is not possible to associate them all together.

  People who send you money cannot see what other bitcoin addresses you own and what you do with them. This is very important advice to keep in mind.

  Use change addresses when you send payments. Certain bitcoin wallet clients, such as bitcoin-Qt, make it difficult to track your transactions by *creating a new change address each time you send a payment*.

For example, if you receive 5 BTC on address A, and you later send 2 BTC to address B, the remaining change must be sent back to you. Some bitcoin clients are designed to send the change to a new address C in such a way that it becomes difficult to know if you own bitcoin address B or C.

- **Be careful with public usage.** Unless your intention is to receive public donations or payments with *full transparency*, publishing a bitcoin address on any public space (i.e. blog, social network, etc.) is not a good idea when it comes to privacy.

  Always remember that when you move any bitcoins from a publicly posted address to one of your non-public wallets, *those bitcoins will be permanently tainted via the blockchain history your publicly posted address*.

  Additionally, it's wise not to publish information about your transactions and purchases that could allow someone to identify your bitcoin addresses.

- **Your IP address is most likely being logged.** Because the bitcoin network is a peer-to-peer network, it is entirely possible to listen for relayed transactions and log their IP addresses.

  Full node clients relay all users' transactions just like their own. This means that finding the source of any particular transaction can be difficult and any bitcoin node can be mistaken as the source of a transaction when they are not.

  Consider masking your computer's IP address with a tool like Tor to help you avoid these undesirable logging issues.

- **Avoid mixing services altogether.** Some online services called mixing services offer to mix traceability between users by receiving and sending back the same amount using independent bitcoin addresses.

  It is important to note that the legality of using such services might vary and be subjected to different rules in each jurisdiction. At best, *such practices are considered sketchy*.

  Also, these types of services require you to extend an **extreme amount of blind faith** in the hopes that the individuals running them will not to lose / steal your funds or keep a log of your requests.

  While mixing services can (theoretically) distort traceability for small amounts... it becomes ever-increasingly difficult to do on a large scale.

Nasty Surfing Habits To Avoid

- Allowing your browser to save your passwords (.vs manually inputting them as needed),

- Staying logged into FaceBook, Google / YouTube, Yahoo, etc. while doing other stuff on the web,

- Not logging out straight away, when finished doing whatever it is you’re doing on these sites,

- Viewing Flash-based media, unprotected (i.e. YouTube, Vimeo, etc),
- Not dumping ALL of your browser's personal data, after each and every web session (no matter how long or short), etc...

How To Break Free From These Nasty Surfing Habits

- **Step 1:** Download Firefox: https://www.mozilla.org/en-US/firefox/new/
- **Step 2a:** Next, get up to speed fast on Comprehensive Firefox security essentials,
- **Step 2b**: And then 10 Ways to Boost Firefox Privacy.
- **Step 2c:** (optional, albeit *highly desirable*) Right click / "save as" the following PDF and absorb it's deep wisdom at your earliest leisure... Collecting, Collating, and Selling Personal Data: Background Information & Research.

Now once you've invoked Step 2a & 2b... The following security / privacy-centric addons are the ones that I personally use & recommend accessorizing your Firefox with:

- **BetterPrivacy:** https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/
- **HTTPS Everywhere:** https://www.eff.org/https-everywhere
- **NoScript:** https://addons.mozilla.org/en-US/firefox/addon/noscript/
- **Ghostery:** https://addons.mozilla.org/en-US/firefox/addon/ghostery/
- **DuckDuckGo:** https://addons.mozilla.org/en-US/firefox/addon/duck-duck-go-ssl/

Important Note: When you initially go through the Ghostery setup wizard, you'll be given numerous options to block certain trackers & cookies. All of them are off (unchecked) by default. Be sure to tick all of them ON for maximum security & privacy from those dirty rat bastards.

Glossary Of Bitcoin Terms

Address: A bitcoin address is similar to an email address. It is the only information you need to provide for someone to *pay you* with bitcoin. Ideally, each address should only be used for one single transaction.

Block: A block is a *permanent record* in the blockchain that contains and confirms many waiting transactions. Approximately every 10 minutes a new block is appended to the blockchain via mining.

Blockchain: The blockchain (or 'block chain') is the shared public ledger on which the entire bitcoin network relies. The blockchain is shared between all bitcoin users and used to archive the permanence of all confirmed bitcoin transactions. Consequently, this is also what prevents double spending.

This way, bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

BTC: The most common abbreviation for bitcoin currency and used in a similar way as USD is used for the US dollar. Occasionally you may also see XBC, bitcoin's other symbol.

Confirmation: A **c**onfirmation means that a transaction has been processed by the network and archived onto the blockchain. A confirmation is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block. Then again for each subsequent block.

A single confirmation is acceptable for low value transactions (<$20). Large amounts (>US$1000) would be wise to wait for at least 6 confirmations. This is because each confirmation *exponentially decreases* the risk of a reversed transaction.

Cryptography: Cryptography is the branch of mathematics that provides high levels of security. In the case of bitcoin, cryptography makes it impossible to spend funds from another user's wallet or to corrupt the blockchain. It is also used to password-protect wallets.

Double Spend: Double spending is when malicious user tries to spend the same bitcoin two different places, back-to-back. Via a combination of bitcoin mining and the blockchain, a *consensus is created on the network* concerning which of the two transactions will be confirmed as valid.

Hash Rate: The hash rate is the measuring unit of the sheer bitcoin network processing power. The hash rate is always proportional to current block difficulty. So as blocks keep getting harder and harder to solve, higher and higher hash rates are required to maintain the network.

For example, when the bitcoin network reached a hash rate of 10 Th/s, it meant it could make 1**0 trillion calculations per second**. These astronomical hash rates consequently keep bitcoin

a safe, fair system for everyone.

Mining: Mining is a distributed consensus system that is used to confirm waiting transactions by entering them into the block chain. Miners enforce a chronological order in the block chain, and protect the integrity and neutrality of the network.

As a reward for their services, bitcoin miners collect modest transaction fees for the transactions they confirm, along with being rewarded newly created bitcoins. The newly created bitcoins are distributed in the equivalent of a *competitive lottery*.

This is what prevents the network from being gamed (i.e. new blocks easily added into the block chain). Consequently, no one can manipulate the block chain (i.e. replacing parts of the block chain to roll back their own spends, etc.)

Mining is also an expensive, highly specialized and competitive **investment** where the rewards are divided up according to how much calculation is done. Consequently, most bitcoin users *do not* mine for bitcoin.

P2P: P2P is the abbreviation for “peer-to-peer” networking and refers to an organized collective that allow individuals to interact directly with each other. In the case of bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users.

Private Key: bitcoin wallets keep a secret piece of data called a private key (aka “seed”), which is used to sign transactions. This secret piece of data is what allows you to spend bitcoins from a given wallet via a cryptographic signature.

Private keys must never be revealed. If an attacker were to discover your private wallet key and transfer those bitcoins elsewhere, it's just the same as if the attacker stole your physical cash.

Signature: A bitcoin signature is a cryptographic means of proving ownership. In the case of bitcoin, a bitcoin wallet and its private keys are cryptographically linked. When your bitcoin software signs a transaction with the correct private key, the network sees that the signature matches the spent bitcoins.

Signatures also prevent transactions from being altered once confirmed. Transactions are broadcast between users and usually receive initial network confirmation in ~10 minutes via Miners.

Transaction: A transaction is a transfer of value between bitcoin wallets that gets confirmed and archived on the blockchain. For transactions to be confirmed, they must be packed in a block that abides by extremely *strict network-verified cryptographic rules*. These rules prevent previous blocks from being modified; as doing so would invalidate all blocks going forward.

Wallet: A bitcoin wallet contains 1 private key and 1 public key; whereas a **wallet client** can contain any number of individual bitcoin wallets.

Closing Thoughts

"However, [governments] don't fear [bitcoin] because of the potential for money laundering, terrorist financing, or harm to unsuspecting consumers. Authorities fear bitcoin *because it threatens the adherence to their fabricated monetary illusion*." [Ed note: emphasis mine]

- Jon Matonis

May your journey into the bitcoin ecosystem be a bold and exciting one!

Best regards,

Mark M. Bravura